Exploit

Cos’è un exploit?

È un codice o una sequenza di comandi ideati per sfruttare una vulnerabilità esistente in un sistema. Gli exploit sono utilizzati per ottenere accesso non autorizzato, eseguire codice dannoso o compromettere la sicurezza del sistema.

Gli exploit possono essere applicati su software come sistemi operativi, applicazioni di produttività, ecc. Per funzionare, richiedono quattro condizioni:

1. Il software deve essere in esecuzione.
2. Non ci devono essere aggiornamenti che risolvano la vulnerabilità sfruttata.
3. L’exploit deve essere progettato per la versione specifica del software.
4. È necessario mantenere la connessione, e bisogna trovarsi nella rete interna.

Exploit: Codice dannoso che sfrutta una vulnerabilità esistente in un programma.

Shell: Rappresenta una connessione diretta con il target, stabilita senza essere rilevati.

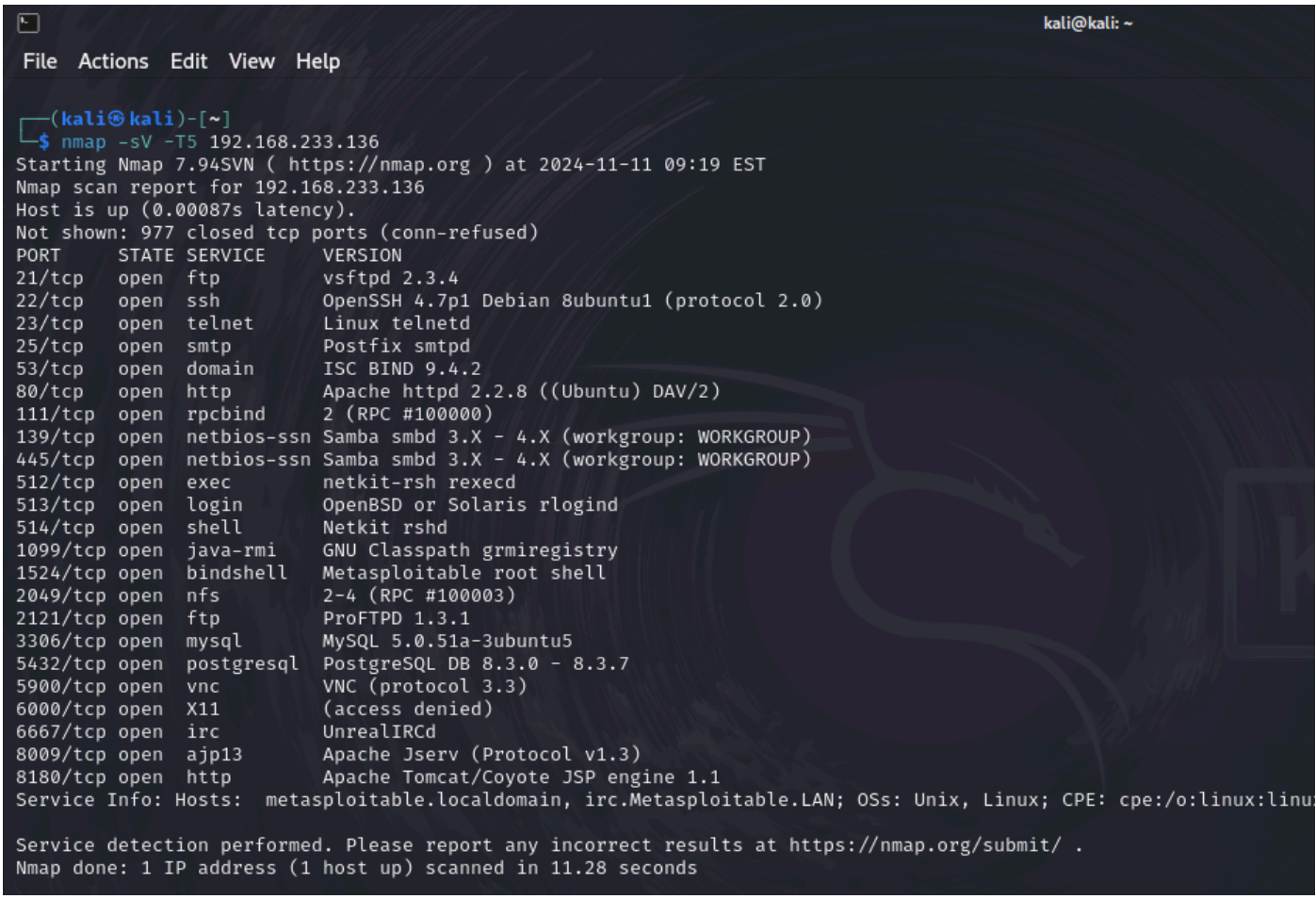
Esercizio:
Hacking con Metasploit Esercizio Traccia
Nella lezione pratica di oggi, ci concentreremo su come condurre una sessione di hacking utilizzando Metasploit su una macchina virtuale Metasploitable.

Traccia dell'Esercizio
Seguendo l'esercizio trattato nella lezione di oggi, vi sarà richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica.

Dettagli dell'Attività Configurazione dell'Indirizzo IP L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable.

Esecuzione esercizio:

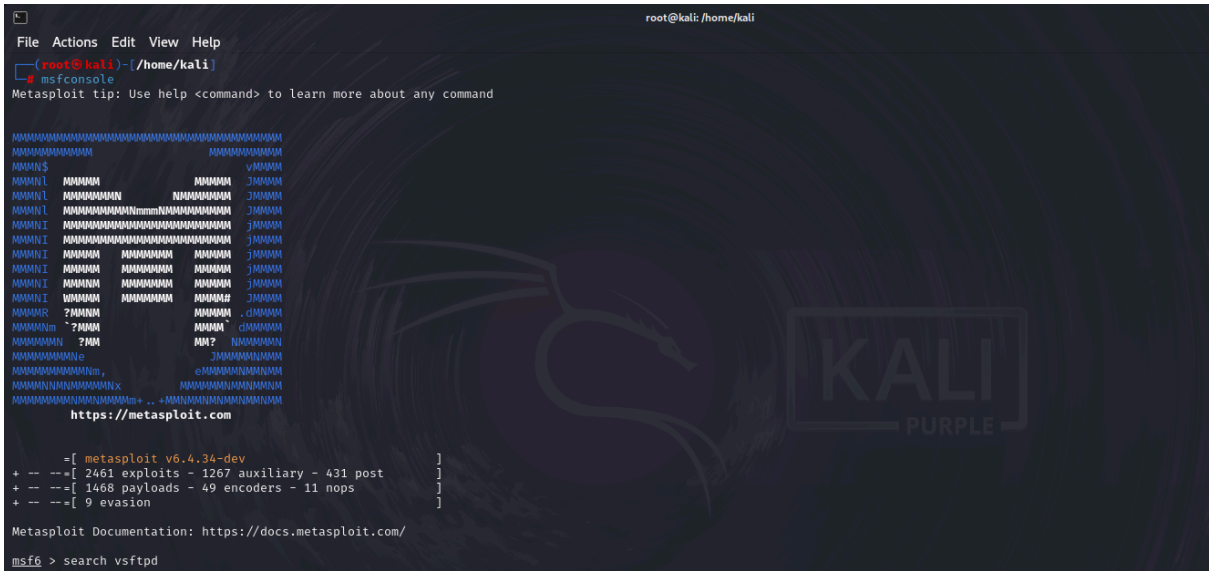
Facciamo una scansione con nmap sull'indirizzo target per visualizzare porte e servizi aperti



Abbiamo visto che la porta 21 è aperta proveremo a eseguire l'attacco proprio su quella porta .

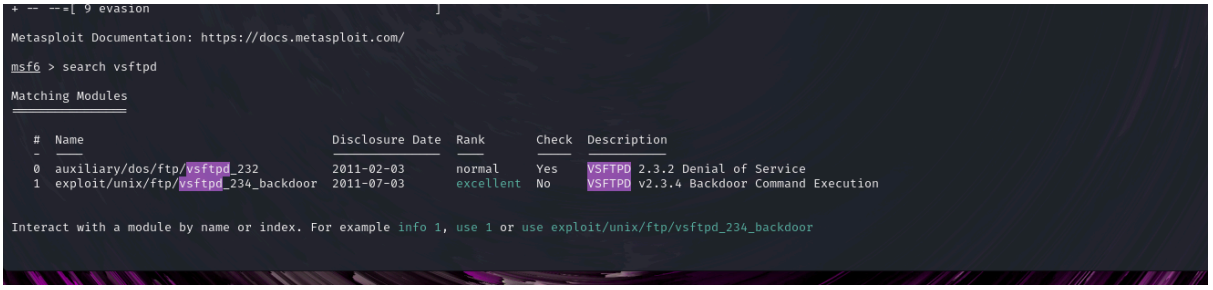
è molto importante tenere conto del servizio he vogliamo attaccare in questo caso la versione è la 2.3.4

Entriamo nella macchina che vogliamo attaccare Metasploite



Cerchiamo l'exploit relativo alla versione del protocollo FTP (vsftpd) usando il comando `SEARCH`, che esegue una ricerca nel database di exploit di Metasploit. Trovati due risultati, selezioniamo il secondo.

Per selezionarlo utilizziamo il comando `USE` con il percorso dell'exploit.

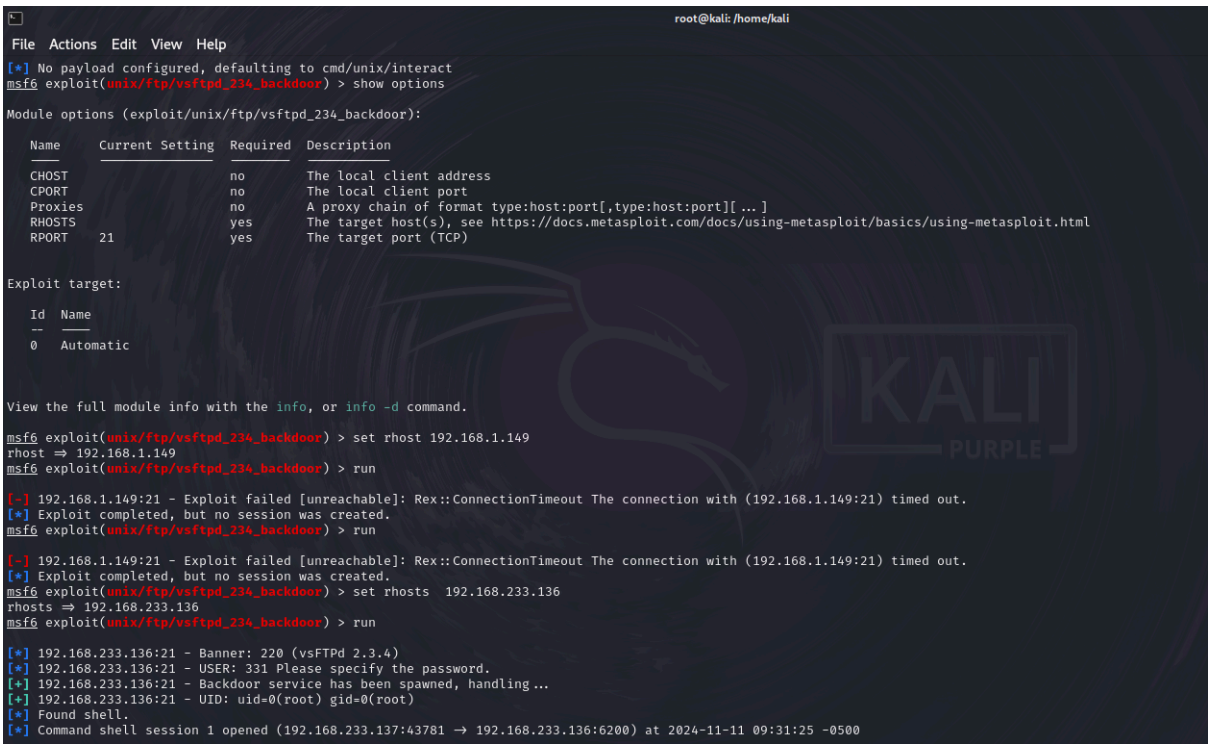


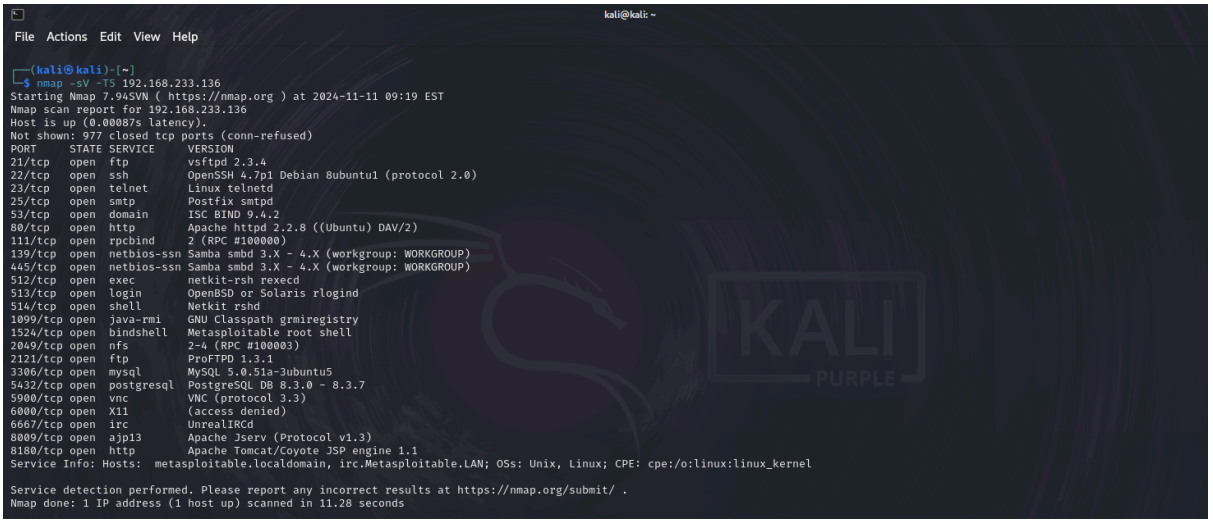
Con `SHOW OPTIONS` visualizziamo i parametri richiesti per l'attacco specifico.

È richiesto l'IP della macchina target, che impostiamo con il comando `SET RHOST 192.168.1.149`.

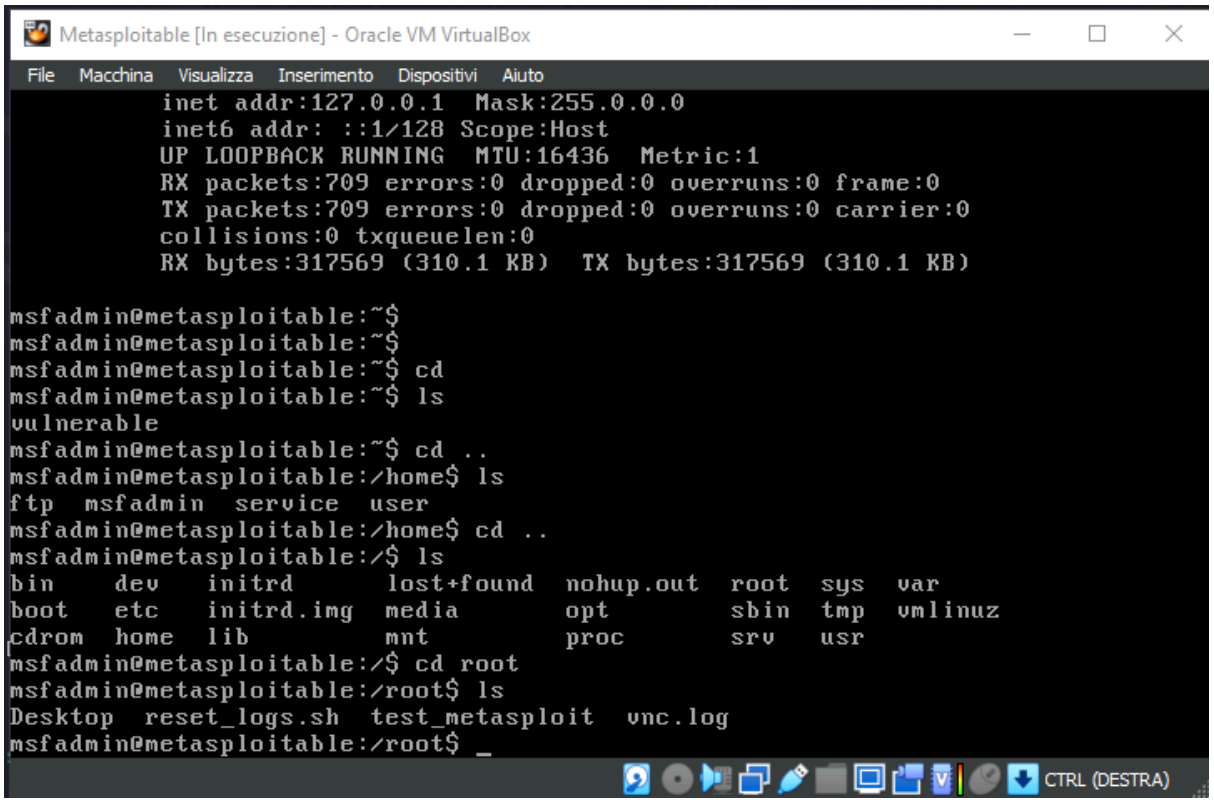
Avviamo l'exploit usando il comando `EXPLOIT` o `RUN`.

Nell'ultima riga viene confermato che il codice dannoso è stato iniettato con successo e che la connessione è stata stabilita.





Procediamo con la creazione della cartella .



Verifichiamo che la cartella sia stata creata .